Chapitre 2- Divisibilité dans $\mathbb{Z}$

Terminales - Maths Expertes

1 Divisibilité

L'arithmétique a pour objet l'étude des nombres entiers.
Ces entiers peuvent être naturels ($\mathbb{N} = \{0,\ 1,\ 2,\ 3,\ \dots\}$) ou relatifs ($\mathbb{Z} = \{\dots,\ -3,\ -2,\ -1,\ 0,\ 1,\ 2,\ 3, \dots\}$)

Définition 1.1.
On considère deux entiers relatifs a et b avec b non nul. On dit que b **divise** a que l'on note $b|a$ s'il existe un entier relatif k tel que $a = k \times b$. on dit également que b est un diviseur de a et que a est un multiple de b.

Exemple :

1. $6 = 2 \times 3$ donc 2 et 3 sont des diviseurs de 6. Les diviseurs dans $\mathbb{N}$ sont 1,2,3,6.
2. $-52 = (-4) \times 13$ donc -4,4,-13 et 13 sont des diviseurs de -52. Les diviseurs de -52 dans $\mathbb{Z}$ sont : -52,-26,-13,-4,-2,-1,1,2,4,13,26,52.

Propriété 1.1.
Conséquences directes

1. 0 est multiple de tout entier a car $0 = a \times 0$.
2. 1 et -1 divisent tout entier a car $a = a \times 1$ et $a = -a \times (-1)$.
3. Si a est un multiple de b et si $a \neq 0$ alors :$|a| \geqslant |b|$.

Propriété 1.2.

1. Soient a et b non nuls, si a divise b et si b divise a alors $a = b$ ou $a = -b$
2. Si c divise b et b divise a alors c divise a.
3. Si c divise a et b alors pour tout entiers relatifs u et v ; c divise $ua + bv$.

Méthode : Utiliser la divisibilité pour résoudre un problème
Comme un entier ne possède qu'un nombre restreint de diviseurs, on cherchera à factoriser et à reconnaître les diviseurs pour résoudre une équation ou un problème de divisibilité.

Exemple :

Déterminer tous les couples d'entiers naturels $(x; y)$ tels que : $x^2 - 2xy = 15$.
On factorise par x : $x^2 - 2xy = 15 \ \Leftrightarrow \ x(x - 2y) = 15$.
On détermine les diviseurs positifs de 15 : $D_{15} = \{1\ ,\ 3\ ,\ 5\ ,\ 15\}$.
Puisque $x > 0$ et $y > 0$, on a $x > x - 2y$. On obtient les décompositions suivantes :

$$\begin{cases} x = 15 \\ x - 2y = 1 \end{cases} \text{ ou } \begin{cases} x = 5 \\ x - 2y = 3 \end{cases} \Leftrightarrow \begin{cases} x = 15 \\ y = \dfrac{x-1}{2} = 7 \end{cases} \text{ ou } \begin{cases} x = 5 \\ y = \dfrac{x-3}{2} = 1 \end{cases}$$

Les couples solutions sont donc : $(15\,;\,7)$ et $(5\,;\,1)$.

Exemple :

Déterminer tous les entiers relatifs n tels que $(n-3)$ divise $(n+5)$.

On a $(n-3)$ divise $(n+5)$,
On a $n-3$ divise $n-3$
donc $n-3$ divise toute combinaison linéaire de $n+5$ et $n-3$ autrement dit $n-3$ divise $n+5-(n-3)=8$
Donc $(n-3)$ est un diviseur de 8.
Les diviseurs relatifs de 8 sont : $D_8 = \{-8\,;-4\,;-2\,;-1\,;\ 1\ ;\ 2\ ;\ 4\ ;\ 8\}$.
On a donc le tableau suivant correspondant aux valeurs possibles de n :

$n-3$	-8	-4	-2	-1	1	2	4	8
n	-5	-1	1	2	4	5	7	11

On vérifie que $(n-3)$ divise bien $(n+5)$ pour toutes ces valeurs de n.

2 La division euclidienne

Théorème 2.1.
Soit a un entier relatif et b un entier naturel non nul.
On appelle **division euclidienne** de a par b, l'opération qui, au couple $(a\ ;\ b)$, associe l'unique couple $(q\ ;\ r)$ tel que :

$$a = bq + r \quad \text{avec} \quad 0 \leq r < b.$$

a s'appelle le **dividende**, b le **diviseur**, q le **quotient** et r le **reste**.

Exemple :

1. La division euclidienne de 114 par 8 correspond à : $114 = 8 \times 14 + 2$.
   Ainsi $q = 14$ et $r = 2$.
2. Pour avoir un reste positif dans la division euclidienne de -114 par 8, on écrit : $-2 = 6 - 8$.
   On obtient alors : $-114 = 8 \times (-14) - 2 = 8 \times (-14) - 8 + 6 = 8 \times (-15) + 6$.
   Ainsi $q = -15$ et $r = 6$.

Remarques

— Le reste est toujours un entier naturel inférieur au diviseur. Par conséquent, dans la division par 7, par exemple, il existe 7 restes possibles : 0, 1, 2, 3, 4, 5, 6.

— On peut schématiser la division euclidienne comme on pose une division : $\begin{array}{r|l} a & b \\ \hline \boldsymbol{r} & \boldsymbol{q} \end{array}$

Ainsi, en reprenant l'exemple de la division de 114 par 8, on a : $\begin{array}{r|l} 114 & 8 \\ \hline \mathbf{2} & \mathbf{14} \end{array}$

Méthode : Utiliser la définition de la division euclidienne

Trouver tous les entiers dont le quotient dans la division euclidienne par 5 donne un quotient égal à 3 fois le reste.

Soit a un entier qui vérifie la condition de l'énoncé. On divise a par 5, on a alors : $a = 5q + r$ avec $0 \leq r < 5$.
Comme $q = 3r$, on a : $a = 15r + r = 16r$ avec $0 \leq r < 5$.

On trouve toutes les valeurs de a en faisant varier r de 0 à 4 compris, on a alors l'ensemble solution : $S = \{0\ ;\ 16\ ;\ 32\ ;\ 48\ ;\ 64\}$.

Exemple :

Lorsqu'on divise a par b, le reste est 8 et lorsqu'on divise $2a$ par b, le reste est 5. Déterminer le diviseur b.

Ecrivons chacune des deux divisions euclidiennes, en notant q et q' les quotients respectifs :

$$\begin{cases} a = bq + 8 \quad \text{avec} \quad b > 8 \\ 2a = bq' + 5 \quad \text{avec} \quad b > 5 \end{cases}$$

En multipliant la première division par 2 et en égalisant avec la deuxième, on obtient :

$$\begin{aligned} 2bq + 16 &= bq' + 5 \quad \text{avec} \quad b > 8 \\ b(2q - q') &= -11 \\ b(q' - 2q) &= 11 \end{aligned}$$

b est donc un multiple positif non nul de 11, supérieur à 8, donc : $b = 11$.

3 Congruence

3.1 Entiers congrus à n

Définition 3.1.
Soit n un entier naturel ($n \geq 2$), a et b deux entiers relatifs.
On dit que deux entiers a et b sont **congrus modulo n** si, et seulement si, a et b ont le même reste dans la division euclidienne par n. On note alors :

$$a \equiv b \mod n \quad \text{ou} \quad a \equiv b\ (n) \quad \text{ou} \quad a \equiv b\ [n].$$

Exemple :

1. $57 \equiv 15\ (7)$ car : $57 = 7 \times 8 + 1$ et $15 = 7 \times 2 + 1$
   $41 \equiv -4\ (9)$ car : $41 = 9 \times 4 + 5$ et $-4 = 9 \times (-1) + 5$
2. Un nombre est congru à son reste modulo n dans la division euclidienne par n.
   $2\,008 \equiv 8\ (10)$ car $2\,008 = 10 \times 200 + 8$; $17 \equiv 1\ (4)$; $75 \equiv 3\ (9)$.
3. Si $x \equiv 0\ (2)$, alors x est pair.
   Si $x \equiv 1\ (2)$, x est impair.

Propriété 3.1. — $a \equiv 0\ (n) \Leftrightarrow a$ est un multiple de n ou n est un diviseur de a.
— La congruence est une relation d'équivalence, c'est-à-dire, pour tous entiers a, b, c, on a :

1. $a \equiv a\ (n)$ (**réflexivité**)
2. Si $a \equiv b\ (n)$, alors $b \equiv a\ (n)$ (**symétrie**)
3. Si $a \equiv b\ (n)$ et si $b \equiv c\ (n)$, alors $a \equiv c\ (n)$ (**transitivité**)

Théorème 3.1.
Soit n un entier naturel ($n \geq 2$), a et b deux entiers relatifs.

$$a \equiv b\ (n) \quad \Leftrightarrow \quad a - b \equiv 0\ (n)$$

Démonstration. Comme il s'agit d'une équivalence, il faut démontrer la propriété dans les deux sens.

— *Dans le sens direct* : On sait que $a \equiv b\ (n)$. Il existe donc des entiers q, q' et r tels que :

$$a = nq + r \quad \text{et} \quad b = nq' + r \quad \text{avec} \quad 0 \leq r < n.$$

On obtient : $a - b = n(q - q')$.$a-b$ est alors un multiple de n, et son reste dans la division par n est nul, d'où : $a - b \equiv 0\ (n)$.

— *Réciproquement* : On sait que $a - b \equiv 0\ (n)$. Il existe k tel que : $a - b = kn \quad (1)$.

Si l'on effectue la division de a par n, on a : $a = nq + r \quad$ avec $\ 0 \leq r < n \quad (2)$.

De (1) et (2), on obtient :

$$\begin{aligned} nq + r - b &= kn \\ -b &= kn - nq - r \\ b &= (q - k)n + r \end{aligned}$$

a et b ont le même reste dans la division par n, donc : $a \equiv b\ (n)$.

CQFD

3.2 Compatibilité de la congruence avec l'addition et la multiplication

Théorème 3.2.
Soit n un entier naturel ($n \geq 2$) et a, b, c, d des entiers relatifs vérifiant :

$$a \equiv b\ (n) \quad \text{et} \quad c \equiv d\ (n).$$

La relation de congruence est compatible :

1. avec l'addition : $a + c \equiv b + d\ (n)$
2. avec la multiplication : $ac \equiv bd\ (n)$
3. avec les puissances : pour tout entier naturel k, $\quad a^k \equiv b^k\ (n)$

Démonstration. 1. **Compatibilité avec l'addition**

On sait que : $a \equiv b\ (n)$ et $c \equiv d\ (n)$, donc $(a - b)$ et $(c - d)$ sont des multiples de n.
Il existe donc deux entiers relatifs k et k' tels que : $a - b = kn$ et $c - d = k'n$.
En additionnant ces deux égalités, on obtient :

$$a - b + c - d = kn + k'n \ \Leftrightarrow \ (a + c) - (b + d) = (k + k')n.$$

Donc $(a + c) - (b - d)$ est un multiple de n, d'où : $a + c \equiv b + d\ (n)$.

2. **Compatibilité avec la multiplication**

On sait que : $a \equiv b\ (n)$ et $c \equiv d\ (n)$, donc, il existe deux entiers relatifs k et k' tels que : $a = b + kn$ et $c = d + k'n$.
En multipliant ces deux égalités, on obtient :

$$\begin{aligned} ac &= (b+kn)(d+k'n) \\ ac &= bd + k'bn + kdn + kk'n^2 \\ ac &= bd + (k'b + kd + kk'n)n \\ ac - bd &= (k'b + kd + kk'n)n \end{aligned}$$

Donc $(ac - bd)$ est un multiple de n, d'où : $ac \equiv bd\ (n)$.

CQFD

Méthodes : Déterminer les restes dans la division euclidienne par 7 des nombres :

1. 50^{100} 2. 100 3. 100^3 4. $50^{100} + 100^{100}$

1. On a $50 \equiv 1\ (7)$ car $50 = 7 \times 7 + 1$.
   D'après la compatibilité avec les puissances, on a : $50^{100} \equiv 1^{100} \equiv 1\ (7)$.
   Le reste est 1.

2. $100 = 50 \times 2$, comme $50 \equiv 1\ (7)$, d'après la compatibilité avec la multiplication, on a : $100 \equiv 2\ (7)$.
   Le reste est 2.

3. Comme $100 \equiv 2\ (7)$, d'après la compatibilité avec les puissances, on a :
   $100^3 \equiv 2^3 \equiv 8 \equiv 1\ (7)$. Le reste est 1.

4. $100^{100} = 100^{3\times 33+1} = (100^3)^{33} \times 100$, donc d'après la compatibilité avec les puissances et la multiplication, on a : $100^{100} \equiv 1^{33} \times 2 \equiv 2\ (7)$.
   D'après la compatibilité avec l'addition, on a alors : $50^{100} + 100^{100} \equiv 1 + 2 \equiv 3\ (7)$.
   Le reste est 3.

Remarque La notion de congruence prend ici tout son intérêt. Par exemple, bien que l'on ne puisse calculer $50^{100} + 100^{100}$, on peut connaître son reste dans la division par 7 de façon simple et rapide.

Méthode : Montrer que : $\forall n \in \mathbb{N},\quad 3^{n+3} - 4^{4n+2}$ est divisible par 11.

On a : $3^{n+3} = 3^n \times 3^3 = 27 \times 3^n$.
Or $27 \equiv 5\ (11)$, donc d'après la compatibilité avec la multiplication, on a :

$$\forall n \in \mathbb{N},\quad 3^{n+3} \equiv 5 \times 3^n\ (11)$$

On a : $4^{4n+2} = (4^4)^n \times 4^2$, or $4^2 \equiv 5\ (11)$ donc $4^4 \equiv 5^2 \equiv 3\ (11)$, donc :

$$\forall n \in \mathbb{N},\quad 4^{4n+2} \equiv 3^n \times 5\ (11)$$

On en déduit donc que :

$$3^{n+3} - 4^{4n+2} \equiv 0\ (11)$$

La proposition est donc vérifiée pour tout entier naturel n.

Méthode : tableau de congruence
Un tableau de congruence est un tableau permettant de présenter des résultats de manière exhaustive en se référant aux restes possibles dans une division euclidienne.

1. Déterminer suivant les valeurs de l'entier relatif n, le reste de la division de n^2 par 7.
2. En déduire alors les solutions de l'équation $x^2 \equiv 2\ (7)$.

1. On détermine les restes suivant une méthode exhaustive, c'est-à-dire on détermine les restes de n^2 à partir de chaque reste possible de la division de n par 7.
   On peut construire un tableau de congruence pour présenter les résultats :

Reste de la division de n par 7	0	1	2	3	4	5	6
Reste de la division de n^2 par 7	0	1	4	2	2	4	1

   Par exemple si $n \equiv 3\ (7)$, alors $n^2 \equiv 9 \equiv 2\ (7)$.
   Les restes possibles de n^2 par 7 sont donc : 0, 1, 2 et 4.
2. Pour résoudre $x^2 \equiv 2\ (7)$, on recherche dans le tableau les valeurs de n pour lesquelles on obtient un reste de 2 quand n est au carré. Il est obtenu pour les restes 3 et 4 dans la division de n par 7.
   Les solutions de l'équation sont donc : $x \equiv 3\ (7)$ et $x \equiv 4\ (7)$.

Définition 3.2.
Soient a un entier relatif et m un entier naturel non nul. On dit que a est inversible modulo m, s'il existe un entier b tel que $a \times b \equiv 1\ (m)$

Exemple :

$8 \times 2 \equiv 1\ (3)$ donc 2 est l'inverse de 8 modulo 3

Exemple :

Calculer le reste de la division euclidienne de 12345^{2000} par 7.
Méthode :
On calcule $12345 \equiv 4\ (7)$ Etablissons la table de congruence de $4^n\ (7)$

Reste de la division de n par 7	0	1	2	3	4	5	6
Reste de la division de 4^n par 7	1	4	2	1	4	2	1

On voit dans le tableau que $4^3 \equiv 1\ (7)$. Décomposons $2000 = 3 \times 666 + 2$
Donc $12345^{2000} \equiv 4^{2000}\ (7) \equiv 4^{3\times 666+2} \equiv (4^3)^{666} \times 4^2\ (7) \equiv 1^{666} \times 16\ (7) \equiv 2\ (7)$ Le reste de la division euclidienne de 12345^{2000} par 7 est 2.